REMARKS

Reconsideration and allowance of the subject application are respectfully requested. Applicant thanks the Examiner for total consideration given the present application. Claims 1-7 were pending prior to the Office Action. No claims have been added through this reply. Claims 6 have been canceled without prejudice or disclaimer of the subject matter included therein. Therefore, claims 1-5 and 7 are pending. Claims 1-2, 4-5, and 7 are independent. Applicant respectfully requests reconsideration of the rejected claims in light of the remarks presented herein, and earnestly seeks a timely allowance of all pending claims.

OFFICIAL ACTION

Preliminary Comments

Request for Initialed/Considered Form PTO-SB08

In reviewing the Examiner's response to the Information Disclosure Statement (IDS) filed on 02/03/2005, Applicants believe that the Examiner is incorrect in his understanding of the IDS filed on 02/03/2005. MPEP 609.04(a), section III, states:

> *Where the information listed is not in the English language, but was cited in a search report or other action by a foreign patent office in a counterpart foreign application, the requirement for a concise explanation of relevance can be satisfied by submitting an English-language version of the search report or action which indicates the degree of relevance found by the foreign office. This may be an explanation of which portion of the reference is particularly relevant, to which claims it applies, or merely an "X", "Y", or "A" indication on a search report.*

The Examiner is incorrect in not considering the IDS filed on 02/03/2005 because the documents were cited in a search report by a foreign patent office in a counterpart foreign application and the requirement for a concise explanation of relevance was (and still is) satisfied

by the submission of an English-language version of the search report which indicated the degree of relevance found by the foreign office, where for example, the English-language version of the search report provides an explanation of which portion of the reference is particularly relevant, to which claims it applies, or merely an "X", "Y", or "A" indication on a search report as required by the MPEP. The Examiner is respectfully requested to review the English-language version of the search report (provided on 02/03/2005) and MPEP 609.04(a), section III, and the Examiner is therefore requested to consider the Information Disclosure Statement submitted on 02/03/2005 and return a copy of the initialed Form PTO-SB08 to the undersigned as soon as possible.

Claim Rejection - 35 U.S.C. § 101

The Examiner rejected claim 6 asserting that claim 6 is not directed to statutory subject matter. By this amendment, Applicant has canceled claim 6. Based on these amendments, it is respectfully requested that the outstanding rejection be withdrawn.

Claim Rejection - 35 U.S.C. § 103(a)

Claims 1-7 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Ko et al. (U.S. Patent 6,597,950) in view of Bates et al. (U.S. Patent Publication 2003/0041315). Applicant respectfully traverses this rejection.

For a Section 103 rejection to be proper, a *prima facie* case of obviousness must be established. *See M.P.E.P. 2142.* One requirement to establish a *prima facie* case of obviousness is that the prior art references, when combined, must teach or suggest all claim limitations. *See M.P.E.P. 2142; M.P.E.P. 706.02(j).* Thus, if the cited references fail to teach or suggest one or more elements, then the rejection is improper and must be withdrawn.

Argument A) Features of claims 1-2, 4-5, and 7 not taught:

In claims 1-2, 4-5, and 7, the Examiner cited the combination of Ko and Bates for the alleged teaching of retrieving an instruction code related to a branch instruction from the data; storing a branch origin address associated with the retrieved instruction code and a branch

destination address associated with a branch destination of the instruction code; judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the branch destination address; storing a call destination address of the instruction code if the instruction code is associated with the branch destination address; and judging whether or not the stored call destination address is between the branch origin address and the branch destination address. The Applicant traverses the rejection based on the combination of Ko and Bates.

The present claimed invention has a feature of detecting data that executes a malicious process by paying attention to an extremely unusual structure (flow of process) which cannot be seen in normal data or programs. More specifically, the present claimed invention does not judge whether or not a malicious process is executed by analyzing a structure or operation of a code which serves execution of a malicious process (for example, a code for generating "stack smashing" or "buffer overflow", but judges whether or not a data is the one that executes a malicious process by checking if there is a flow of processes in data, which intentionally executes such a malicious code. In the present claimed invention, a code is not judged as a malicious code by simply analyzing a branch structure of data and also by the result of the analysis that the code to be executed later precedes the code being currently executed.

The unique structure of the present claimed invention is not disclosed or suggested by cited references Ko, Bates, and Baratloo, that is, data which executes a malicious process is detected by paying attention to an unusual structure in data leading to a malicious code.

Ko merely discloses a structure wherein a macro operation is extracted from a received document (Fig. 3, element 304), a static analysis is performed on the extracted macro operation (Fig. 3: 306) and the macro operation is judged if it is suspicious or not (Fig. 3, element 308). That is, Ko examines the actual performance of the macro operation contained in the received document so as to detect a suspicious macro operation, and does not describe that a suspicious macro operation is detected by a flow of process leading to a program code describing the macro operation. Therefore, Ko is different from the present claimed invention.

Baratloo merely discloses specific examples of an execution code for generating "stack smashing" or "buffer overflow". Therefore, if a structure or operation of an execution code

contained in data is concretely examined according to the teaching of Baratloo, it may be possible to judge whether or not the data is data that executes a malicious process. However, Baratloo does not describe or suggest an unusual structure in data which intentionally executes the above mentioned execution code. Therefore, Baratloo does not provide a solution to the problem as to how to detect subspecies of the execution codes shown as examples in Figs. 3 to 5, or other malicious codes.

To the contrary, the present invention, based on a flow of process leading to a malicious code, it is judged whether or not the data is data that executes a malicious process is executed. Thus, the present invention is apparently different from Baratloo.

On the other hand, Bates discloses a technique for analyzing a branch structure, which is a technique relating to debug for software. The Examiner points out that "judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address" is described in paragraph [0048] of Bates. However, CDSet158 and BranchSet156 described in Bates are merely provided with a function for storing a basic block and a function for storing a branch address, respectively, and thus they do not have a function of judgment.

Also, in Bates, it is only needed to find out control dependency between the basic blocks. It is not necessary to distinguish if a transition between the basic blocks is caused by a jmp instruction or by a call instruction. Therefore, Bates has no motivation for "judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address" or "judging whether or not the stored call destination address is between the branch origin address and the branch destination address".

That is, Bates lacks the structures which are specified matters of the present claimed invention, namely, the structure for "judging whether or not an instruction code for calling an instruction code group for executing a predetermined process is associated with the stored branch destination address" and the structure for "judging whether or not the stored call destination address is between the branch origin address and the branch destination address". Thus, Bates does not disclose the features relied upon for the present claimed invention.

Accordingly, even if Bates is applied for cited reference Ko and cited publication Baratloo, it is impossible for realize the effect of the present claimed invention, that is, judging whether or not data is the date on which a malicious process is executed by an unusual structure (flow of process) in data leading to a malicious code.

The present claimed invention has a feature of detecting data that executes a malicious process by paying attention to an extremely unusual structure (flow of process) which cannot be seen in normal data or programs and by examining if a flow of process exists in data, which intentionally executes a malicious process.

In the present invention, it is possible to judge whether or not data is the data which executes a malicious process, without examining the structure of the malicious code itself. This realizes the specific effect of the present invention which cannot be expected by references, that is, detection of a malicious code is possible through a flow of process leading to the malicious code, even after the malicious code has been altered or subspecies thereof has been generated.

Thus, claims 1-2, 4-5, and 7 are submitted to be allowable over the cited prior art for at least this reason.

Dependent claim 3 is allowable for the reasons set forth above with regards to claim 2 at least based on their dependency on claim 2.

Accordingly, Applicants respectfully request that the Examiner reconsider and withdraw the rejection of claims 1-5 and 7 under 35 U.S.C. § 103(a).

Reconsideration and allowance of claims 1-5 and 7 are respectfully requested for at least these reasons.

Conclusion

Therefore, for at least these reasons, all claims are believed to be distinguishable over the combination of Ko and Bates, individually or in any combination. It has been shown above that the cited references, individually or in combination, may not be relied upon to show at least these features. Therefore, claims 1-5 and 7 are distinguishable over the cited references.

In view of the above amendments, it is believed that the pending application is in condition for allowance.

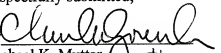
Applicant respectfully requests that the the pending application be allowed.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Aslan Ettehadieh Reg. No. 62,278 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.147; particularly, extension of time fees.

Dated: August 26, 2008

Respectfully submitted,

By 
Michael K. Mutter #2927
Registration No.: 29,680
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant